REMARKS

This is in response to the Office Action dated April 28, 2010. In view of the above amendments and the following remarks, reconsideration of the rejection and further examination are requested.

Rejection under 35 U.S.C §112, second paragraph

Claims 1-36, 39-40 and 42 have been rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. This rejection is submitted to be inapplicable to the claims, as amended, for the following reasons.

Independent claims 1, 14, 25, 39, 40, and 42 have been amended to recite that "the pieces of new unique information" are "derivatively obtained from the pieces of unique information." This amendment clarifies that, although the information is new, the new unique information is derived from the unique information.

Claims 2-13 are either directly or indirectly dependent on independent claim 1. Claims 15-24 are either directly or indirectly dependent on independent claim 14. Claims 26-36 are either directly or indirectly dependent on independent claim 25. As a result, it is submitted that claims 1-36, 39-40 and 42 are now in compliance with 35 U.S.C. §112, second paragraph.

Rejection under 35 U.S.C §103(a):

Claims 1-36, 39-40, and 42 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Asano (US 7,088,822) in view of Lotspiech (US 7,010,125). This rejection is submitted to be inapplicable to the claims, as amended, for the following reasons.

Claim 1 recites a second assignment unit operable to bring, for a subset being an association source generated for a node in one of the layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence, respectively, with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in the one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source, the prescribed operation being to generate corresponding decryption keys and generate the pieces of new unique information derivatively obtained from the pieces of unique information.

According to the above structure as recited in claim 1, two sub-trees rooted at two nodes in a parent-child relationship can be associated with each other. Specifically, a subset F1 in a plurality of subsets generated in a sub-tree whose root is the child node is associated with a subset F2 containing the subset F1 in a plurality of subsets generated in a sub-tree whose root is the parent node. This makes it possible to associate subsets contained in two different sub-trees with each other, thus decreasing the number of unique information pieces to be distributed. The combination of Asano and Lotspiech fails to disclose the above features as recited in claim 1.

As discussed in the amendment filed on January 27, 2010, Asano discloses a technique for performing key management by means of a tree structure. In the key management of Asano, each leaf in the tree structure is assigned to a playback apparatus, and each node is assigned to a key. Since the keys do not depend on one another, it is necessary for the playback apparatus to manage all of the keys existing in all paths from the root to the apparatus. Thus, the tree structure described in Asano becomes very complicated due to the large number of layers. This is because as the number of playback apparatuses increases, the number of keys assigned to each playback apparatus increases. For example, Asano discloses that a device 0 would possess leaf key K0000 and node keys K000, K00, K0, and KR (see col. 20, lines 12-20). This method results in a complicated tree structure, which causes an increase in the number of playback apparatuses that manage the keys and an increase in the number of keys assigned to each playback apparatus. Asano also discloses the relations among the indexes 0, 00, 000 and that keys assigned to the indexes 00, 0 are separately obtained from encrypted data corresponding to the index 000 one by one, as shown in Figure 12 (see col. 21, lines 25-49).

However, Asano does not disclose associating the subset, belonging to the lowermost layer, with the subset, belonging to an immediately upper layer, and assigning new pieces of unique information, derivatively obtained from pieces of unique information assigned to a subset belonging to one of the layers, to another subset with which the subset is associated. This is different from Asano because in claim 1 the pieces of unique information are assigned to two subsets that are associated with each other (i.e., one subset in one of the layers and another subset positioned in an immediately upper layer).

Therefore, Asano does not disclose or suggest a second assignment unit operable to bring, for a subset being an association source generated for a node in one of the layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence, respectively, with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in the one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source, the prescribed operation being to generate corresponding decryption keys and generate the pieces of new unique information derivatively obtained from the pieces of unique information, as recited in claim 1. Lotspiech also fails to disclose or suggest the above features as recited in claim 1.

Lotspiech discloses that the system is initiated by supplying each receiver with private information I_u useful for decrypting content (see col. 4, lines 66-67). If I_u is the secret information provided to receiver u, then each receiver u in S_j can deduce L_j from its I_u (see col. 5, lines 2-4). Thus, subset keys L, for a subset defined by the subset difference, are derived using private information I_u supplied to each receiver belonging to the subset. However, similarly to Asano above, Lotspiech does not disclose assigning new private information derived from the private information supplied to the subset defined by a subset difference to another subset that wholly contains the subset and is made up of the smallest number of elements. Therefore, it is apparent that Lotspiech fails to disclose or suggest the features lacking from Asano discussed above with regard to independent claim 1. Accordingly, no obvious combination of Asano and Lotspiech would result in, or otherwise render obvious under 35 U.S.C. §103(a), the features recited in claim 1. Therefore, claim 1 is patentable over the combination of Asano and Lotspiech.

Claim 25 is patentable over the combination of Asano and Lotspiech for the same reasons as those discussed above with regard to independent claim 1. Specifically, claim 25 recites a second assignment unit operable to bring pieces of new unique information into correspondence with subsets other than the subset that has the smallest number of elements respectively and assigns each piece of new unique information to one or more apparatus identifiers that are contained in each of said other subsets, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset that has the smallest number of elements respectively , the prescribe operation being to generate corresponding decryption keys and generate the pieces of new unique information derivatively obtained from the pieces of unique information. As discussed above, the combination of Asano and Lotspiech fails to disclose or suggest the above features of claim 25. For at least this reason, claim 25 is patentable over the combination of Asano and Lotspiech.

Claims 40 and 42 are patentable over the combination of Asano and Lotspiech for reasons similar to those discussed above with regard to claim 1. Specifically, claims 40 and 42 recite a second assignment step of bringing for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence, respectively, with the one or more subsets being association destinations and assigning the pieces of new unique information to apparatus identifiers contained in the one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of new unique information corresponding to the subset being an association source, the prescribed operation being to generate corresponding decryption keys and generate the pieces of new unique information derivatively obtained from the pieces of unique information. As discussed above, the combination of Asano and Lotspiech fails to disclose or suggest the above features of claims 40 and 42. For at least this reason, claims 40 and 42 are patentable over the combination of Asano and Lotspiech.

Claim 14 contains features directed to performing a second assignment for bringing, for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source , the prescribed operation being to generate corresponding decryption keys and generate the pieces of new unique information derivatively obtained from the pieces of unique information. As discussed above, the combination of Asano and Lotspiech fails to disclose or suggest the above features of claim 14. For at least this reason, claim 14 is patentable over the combination of Asano and Lotspiech.

Claim 39 is not anticipated by Asano for reasons similar to those discussed above with regard to independent claim 1. Specifically, claim 39 recites an integrating unit operable to, after the second control unit performs the processing on all of the layers, integrate into one group (i) a lower-layer group and (ii) an upper-layer group that includes a subset that wholly contains one of subsets belonging to the lower-layer group and that is generated for a parent node of a node for which the one of subsets are generated, the lower-layer group and the upper-layer group belonging to mutually different layers, and a second assignment unit operable to bring pieces of new unique information into correspondence with subsets other than the subset that has the smallest number of elements respectively and assigns each piece of new unique information to one or more apparatus identifiers that are contained in each of said other subsets, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset that has the smallest number of elements, respectively, the prescribed operation being to generate corresponding decryption keys and generate the pieces of new unique information derivatively obtained from the pieces of unique information. Similarly to claim 1 discussed above, the above features as recited in claim 39 make it is possible to associate, in two sub-trees whose roots are respectively a parent node and a child node in a parent-child relationship, a subset Fl in a plurality of subsets generated in a sub-tree whose root is the child node with a subset F2 including the subset F1 in a plurality of subsets generated in a sub-tree whose root is the parent node. This makes it possible to associate subsets included in two different sub-trees with each other, that is, to associate different sub-trees with each other, thereby decreasing the number of the unique information pieces to be distributed.

As noted above, the combination of Asano and Lotspiech does not disclose the association of a subset in a plurality of subsets generated in a sub-tree whose root is the child node with a subset including the subset in a plurality of subsets generated in a sub-tree whose root is the parent node. Therefore, claim 39 is patentable over the combination of Asano and Lotspiech.

Claims 2-13 are either directly or indirectly dependent on independent claim 1. Claims 15-24 are either directly or indirectly dependent on independent claim 14. Claims 26-36 are either directly or indirectly dependent on independent claim 25. As a result, claims 1-36, 39-40, and 42 are allowable over the combination of Asano and Lotspiech.

Because of the above-mentioned distinctions, it is believed clear that claims 1-36, 39-40, and 42 are allowable over the reference relied upon in the rejection. Furthermore, it is submitted that the distinctions are such that the present invention, as recited in claims 1-36, 39-40, and 42, would not have been obvious to a person having ordinary skill in the art at the time of the invention. Therefore, it is submitted that claims 1-36, 39-40, and 42 are clearly allowable over the prior art of record.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance. The examiner is invited to contact the undersigned by telephone if it is felt that there are more issues remaining which must be resolved before allowance of the application.

Respectfully submitted,

Toshihisa NAKANO et al.

/Allen N. Doyel/
By 2010.07.26 15:59:54 -04'00'

Allen N. Doyel
Registration No. 60,391
Attorney for Applicants

AND/MSH/ats
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 28, 2010